This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Optimal Surveillance Schedule Based on Mobile ID Check technology

Simulation: OMNeT++ 5.0/INET3.4

Ali Alshawish
Amine Abid
Herman de Meer

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

2nd HyRiM End User Workshop
Barcelona, 15.11.2016

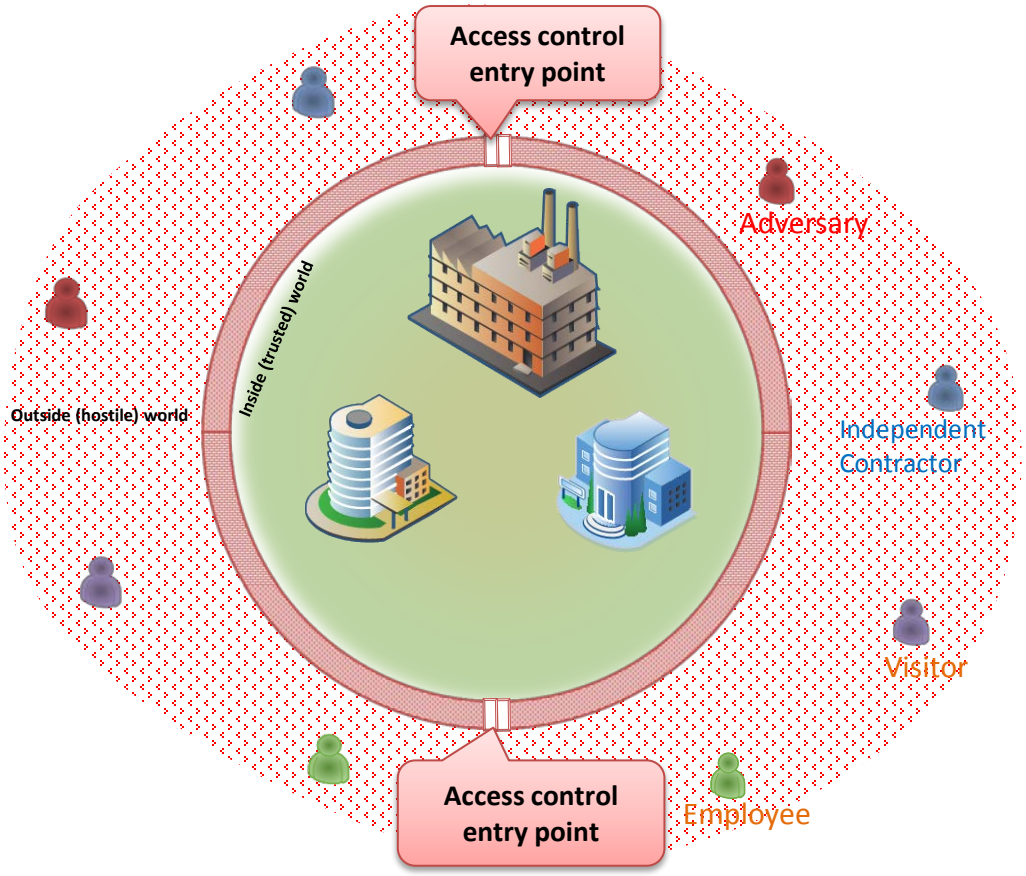
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Contents

- General Context
- Defender / Attacker Strategies
- Solving a Multi-objective Security Game Model
  - Gathering Data
  - Optimal Defense Strategy
  - Worst-case attack Strategy

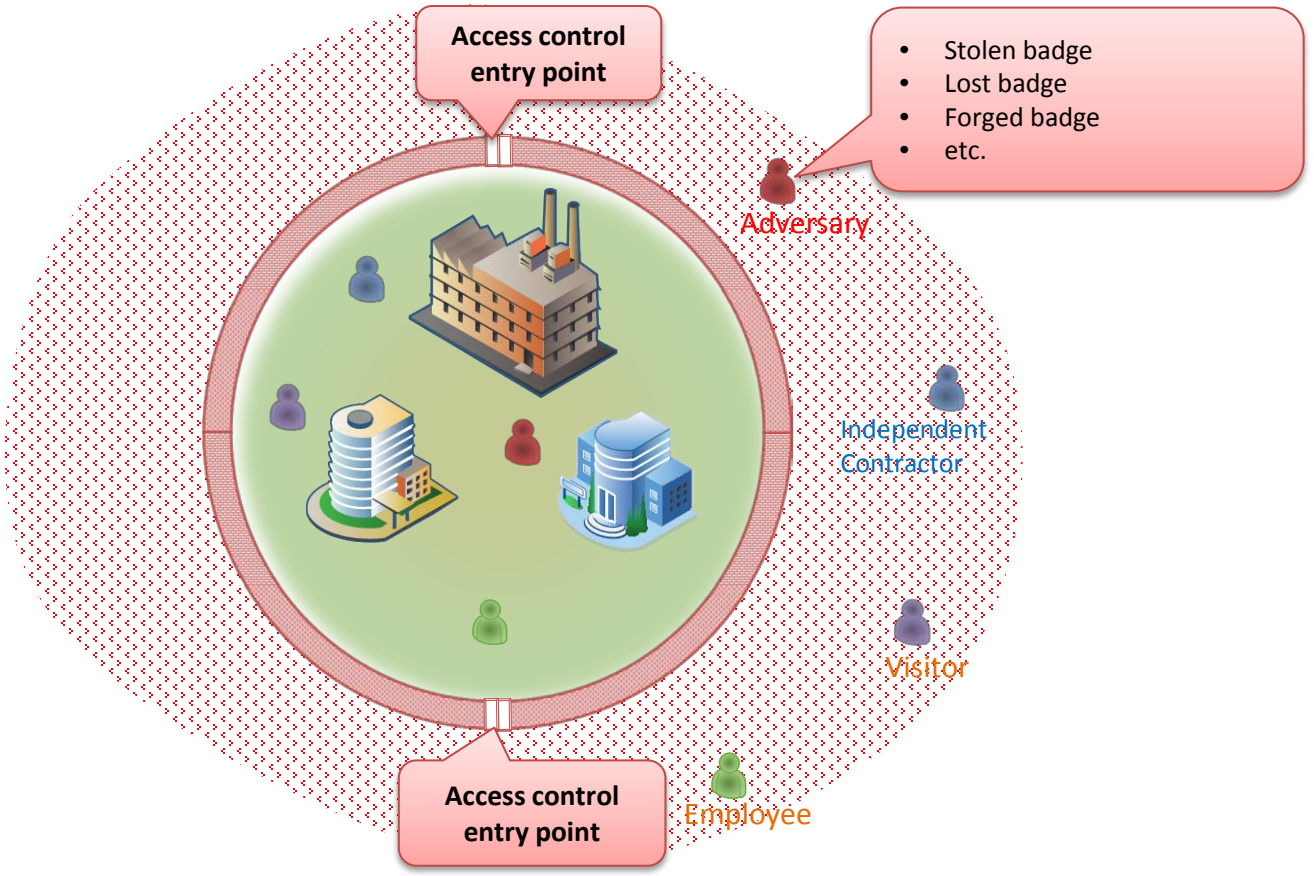
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

General Context (1/3)



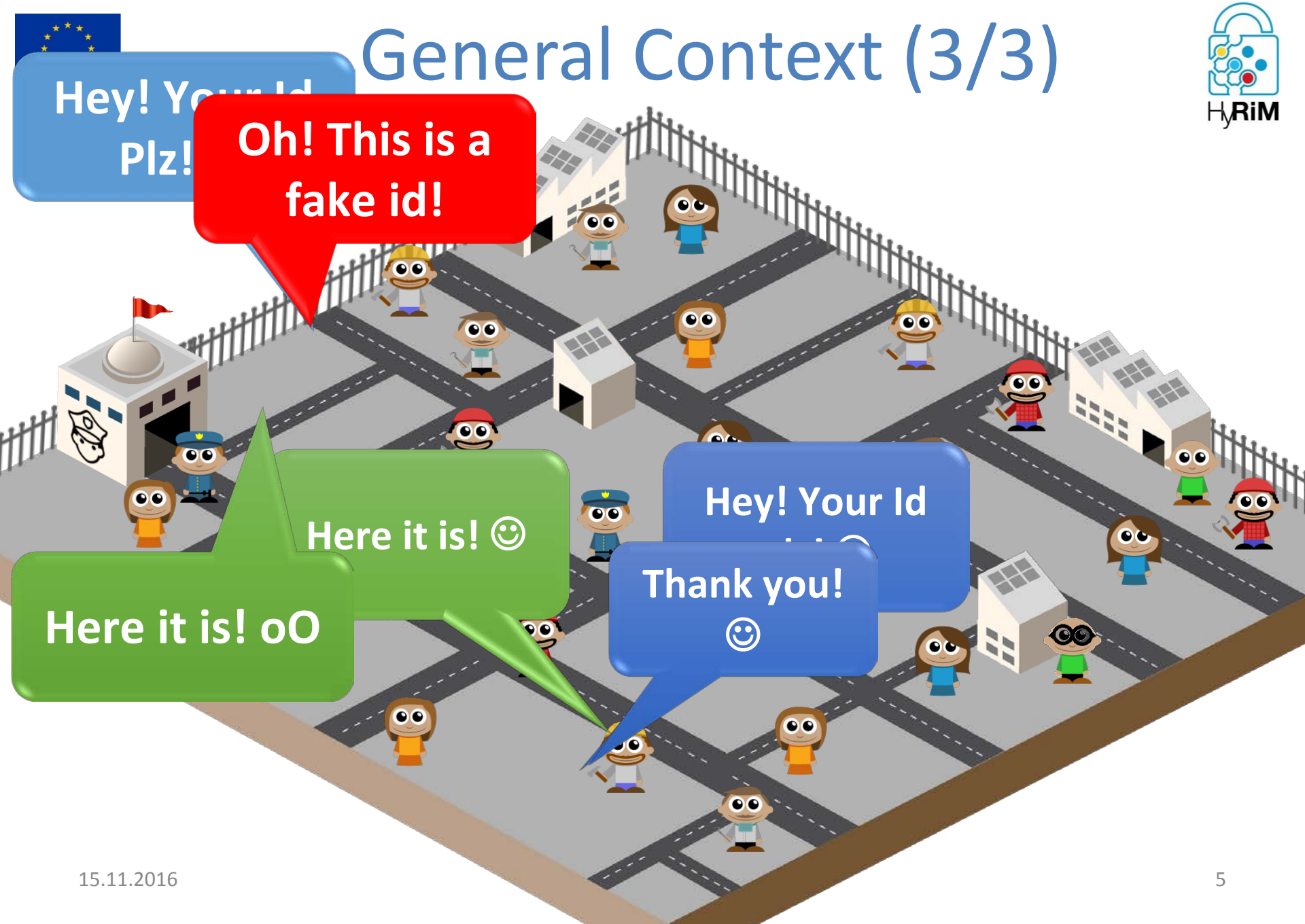
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090

General Context (2/3)



- There is still a way **In**! ➔ *extend* surveillance to the *inside*: **Mobile ID-Check**

General Context (3/3)



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Strategies (1/2)

- Defender strategies:
  - Not one single way to perform mobile ID checking: many different strategies?
    - Number of security guards
    - Missions duration
    - Missions frequency
    - How to select which area to visit now?
- Attacker strategies:
  - Attackers may also have different strategies!
    - Number of intruders
    - How to target areas
    - …
- What is the best defense strategy to apply with respect to several objectives?
  - Multi-goal security strategy (MGSS)

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Strategies (2/2)

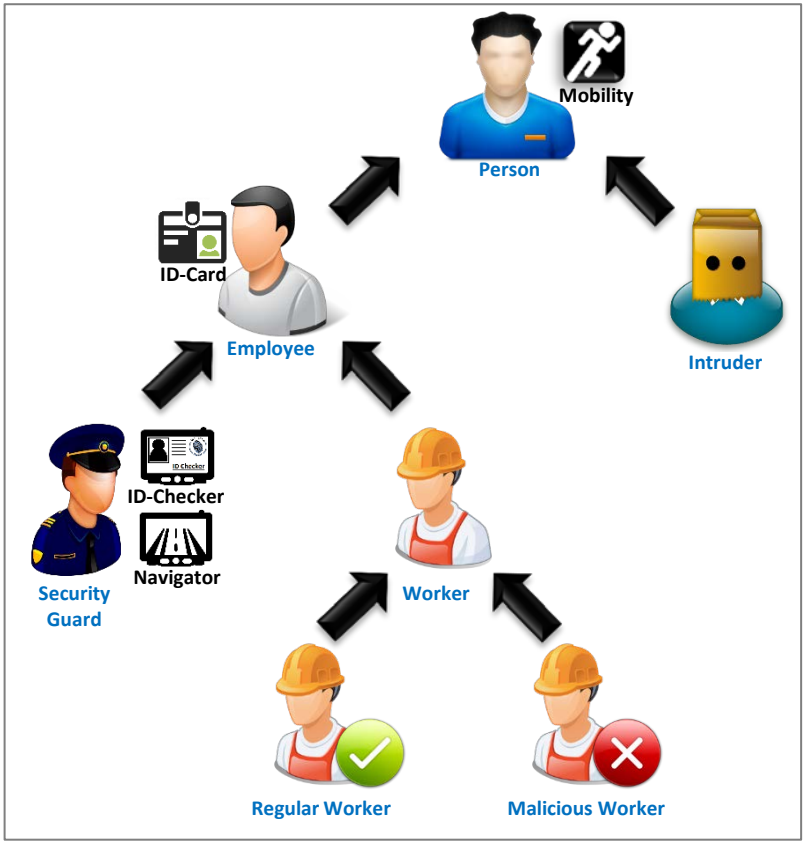
- Construct and solve a multi-objective security game model
  - Gather data ← Simulation Platform for Mobile ID-check operations
  - Compile loss distributions
  - Prioritize the goals
  - Find the equilibrium
    - The optimal defense strategy
    - The worst case attack strategies for each identified goal

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulation Actors

- Every employee has an ID-Card (known to the system)
- Security Guards are equipped with mobile ID-Check Devices (detects threats for sure upon a check)
- An intruder is a person holding a fake ID-Card (not known to the system)
- An employee is either Malicious or Regular (can be detected if he shows odd behavior)
- A Malicious employee/intruder can only be detected upon a check

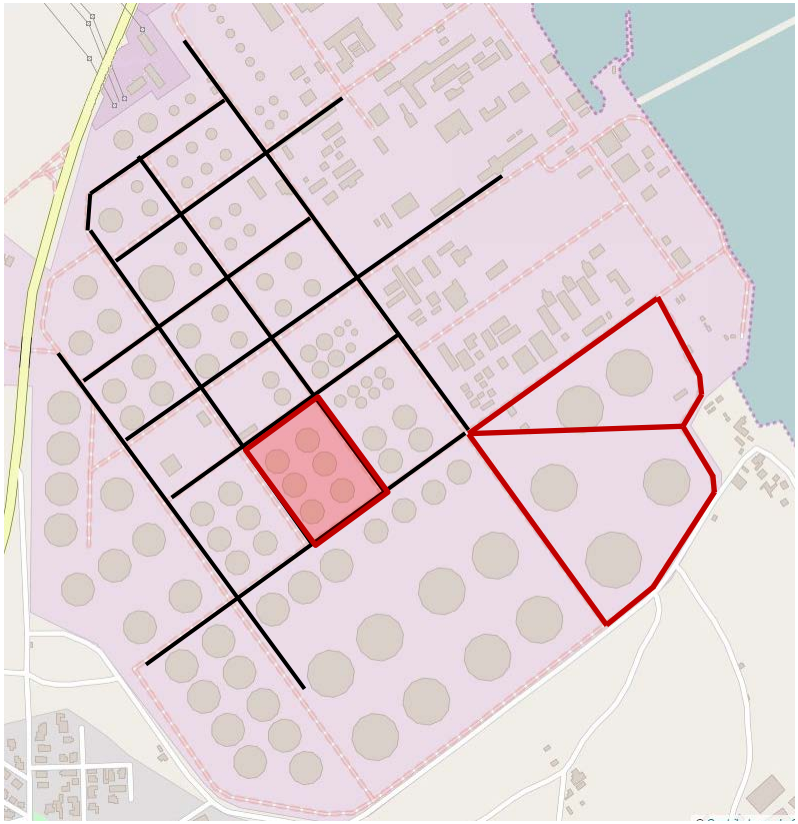


This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulated Environment

- The facility is divided into several areas
- Each area has a security level
  - The higher, the bigger is the caused damage by an attack
- To navigate from one area to another, we follow fixed paths.
- Movement inside an area is random (RWP model)



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Targeted Goals (Key Performance Indicators)

- Average*[/Max/Min]* privacy breach:
  - Maximum individual privacy breach experienced by the workers
- Average*[/Max/Min]* number of checks:
  - Average number of times a worker has been checked
- Average*[/Max/Min]* Number of visits per area
  - How many times an area is visited by a security guard in average
- Average*[/Max/Min]* mission duration
  - How much time a checking mission lasts in average
- Average*[/Max/Min]* inter-mission duration
  - How much time spent between two successive missions in average
- Detection rate
  - Number of detected intruders/Total number of intruders
- Average*[/Max/Min]* caused damage
  - $\frac{1}{NI}\sum_i \sum_j timeSpent(intruder_i, area_j) \times secLevel(area_j)$
  - Where NI is the number of intruders
- Average*[/Max/Min]* time spent before being caught
  - Average time spent by an intruder before being caught by a security guard

Preserve Privacy / Reduce privacy breach

Increase Security

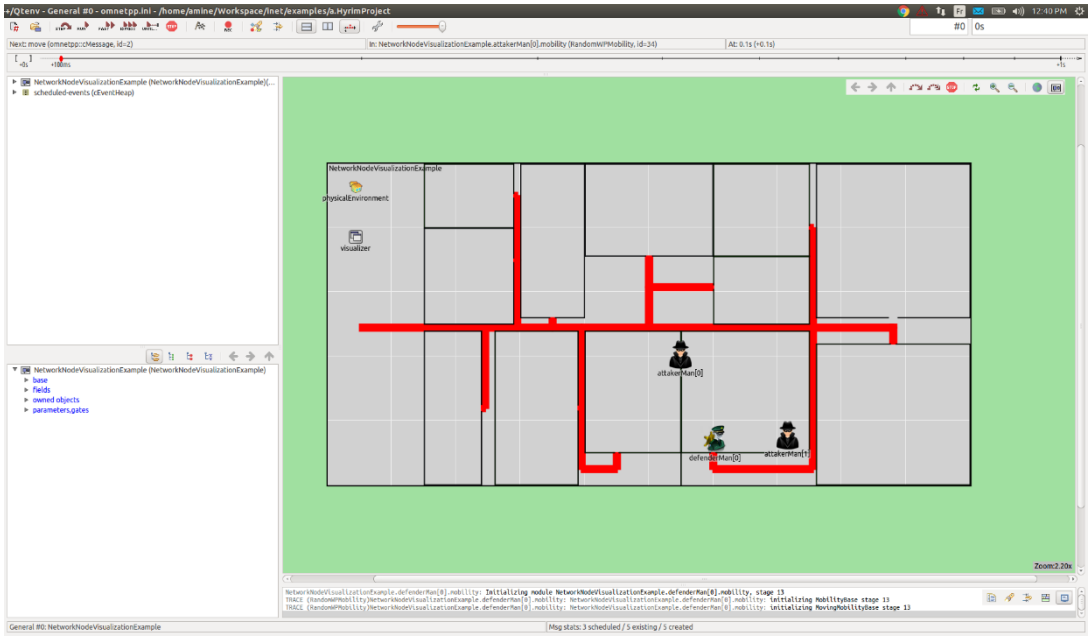
Reduce Caused Damage

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulation Set Up (1/3)

- Simulation Time:
  - 8 working hours
- 12 Areas
- 60 Employees
  - all regular
- Check time
  - uniform(20sec, 1min)
- Sec. levels:
  - #4 Areas – sec. level 2
  - #6 Areas – sec. level 5
  - #2 Areas – sec. level 7



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulation Set Up (2/3)

Defender Strategies:

- Number of security Guards: 1..5 - all regular
- Missions duration:
  - uniform(5min, 15min)
- Missions frequency:
  - 1, 3, 5 spread uniformly over the working hours
- How to select which area to visit now?
  - Choose randomly
  - The higher the security level, the most probably the area is selected

6 defender strategies

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulation Set Up (3/3)

Attacker Strategies:

- Number of intruders: 1, 5, 10
- How to select which area to target now?
  - Choose randomly

3 Attacker strategies

Number of runs per scenario: 5

➔ Total number of runs: 6 x 3 x 5 = 75 runs

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

Simulation Results (1/2)

- 3 defender strategies
  - D-NG1F7TR: 1 sec. guard, freq = 7 & areas: targeted randomly
  - D-NG3F7TR: 3 sec. guards, freq = 7 & areas: targeted randomly
  - D-NG5F7TR: 5 sec. guards, freq = 7 & areas: targeted randomly
  - D-NG1F7THSLF: 1 sec. guards, freq = 7 & areas: targeted higher sec. lev. First
  - D-NG2F7THSLF: 3 sec. guards, freq = 7 & areas: targeted higher sec. lev. First
  - D-NG5F7THSLF: 5 sec. guards, freq = 7 & areas: targeted higher sec. lev. first
- 3 attacker strategies
  - A-NI1TR: 1 intruder & areas are targeted randomly
  - A-NI5TR: 5 intruders & areas are targeted randomly
  - A-NI10TR: 10 intruders & areas are targeted randomly

This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Gathering Data

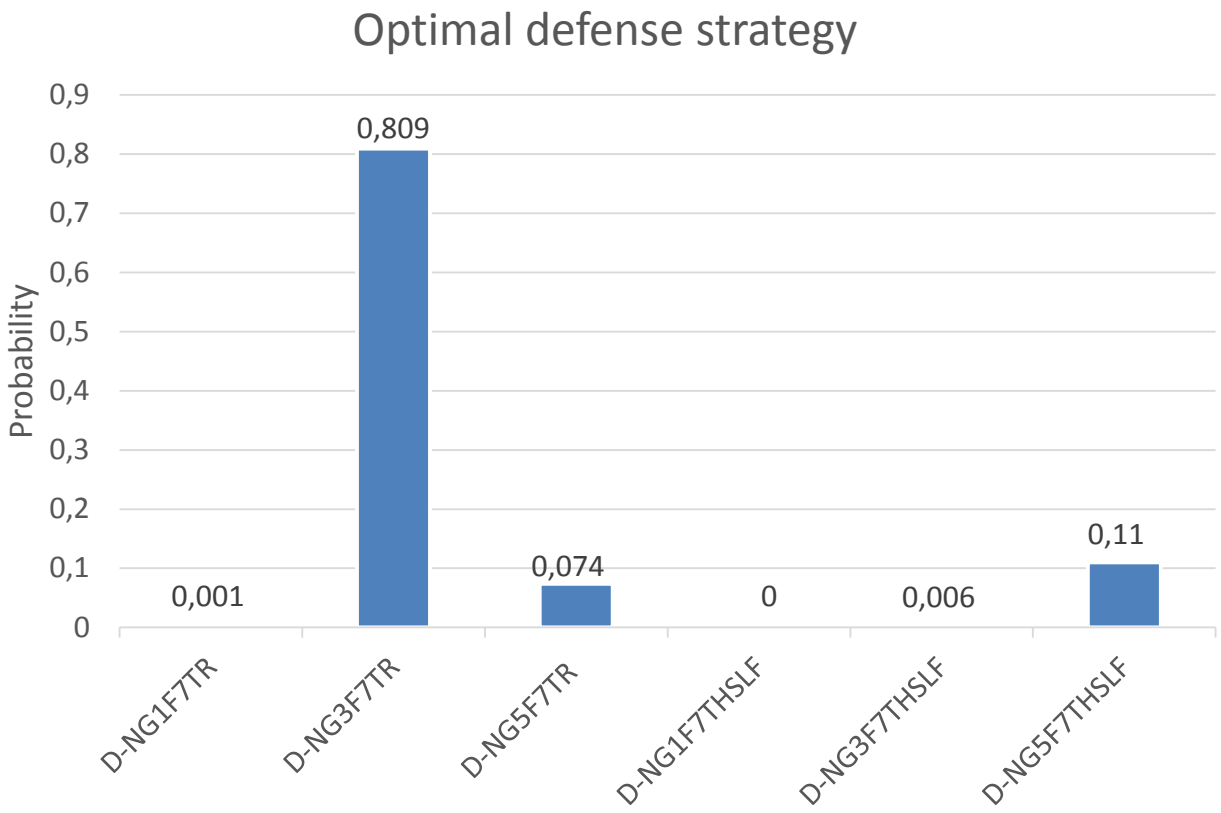
Simulation Results (2/2)

			A-NI1TR					A-NI5TR					A-NI10TR				
			Run #														
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
D-NG1F7TR	KPIs	Max. Privacy	1	2	1	1	1	1	2	1	1	2	1	1	1	3	1
		Damage	3	3	3	3	3	2	3	3	2	2	2	2	3	2	2
		Detec. Rate	1	1	1	1	1	2	1	1	3	1	1	3	1	2	1
D-NG3F7TR		Max. Privacy	2	1	2	3	2	3	2	1	1	2	2	2	2	3	2
		Damage	1	2	2	1	2	2	2	2	2	3	2	2	2	2	2
		Detec. Rate	5	1	1	5	1	1	3	2	3	1	4	2	2	2	2
D-NG5F7TR		Max. Privacy	3	3	2	3	4	3	3	4	3	4	5	5	4	2	3
		Damage	2	2	3	1	1	2	2	2	1	2	3	2	2	2	1
		Detec. Rate	1	1	1	5	5	4	2	3	3	5	1	3	3	3	4

1	2	3	4	5
very low	low	medium	high	very high

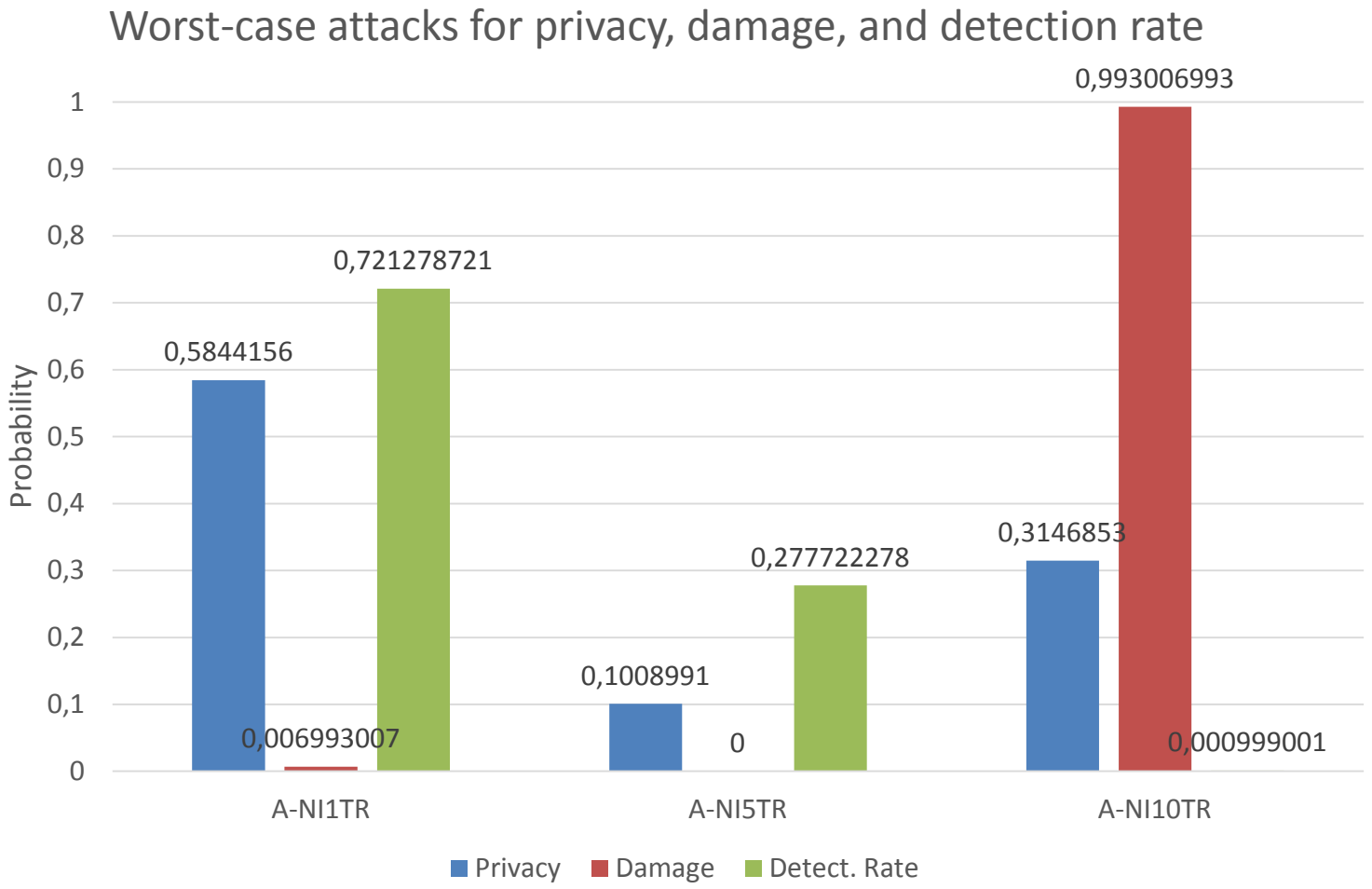
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Optimal Defense Strategy



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

Worst-case Attack Strategy



This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608090.

HyRiM

Questions?

Optimal Surveillance Schedule Based on Mobile ID Check technology

Simulation Part: OMNeT++ 5.0/INET3.4

Ali Alshawish
Amine Abid
Herman de Meer

UNIVERSITÄT PASSAU
Fakultät für Informatik und Mathematik

2nd HyRiM End User Workshop
Barcelona, 15.11.2016